FIM (ファイル整合性監視)

FIM (ファイル整合性監視)

Pandora FMS ドキュメント一覧に戻る

概要

ファイル整合性監視 (FIM) を使用すると、設定ファイルなどの重要なファイルがシステム内でいつでも変更されたかどうかを確認できます。

Pandora FMS では、バージョン 784 以降Linux® と MS Windows® システムの両方で、これらの監視機能を エンドポイント に組み込んでいます。

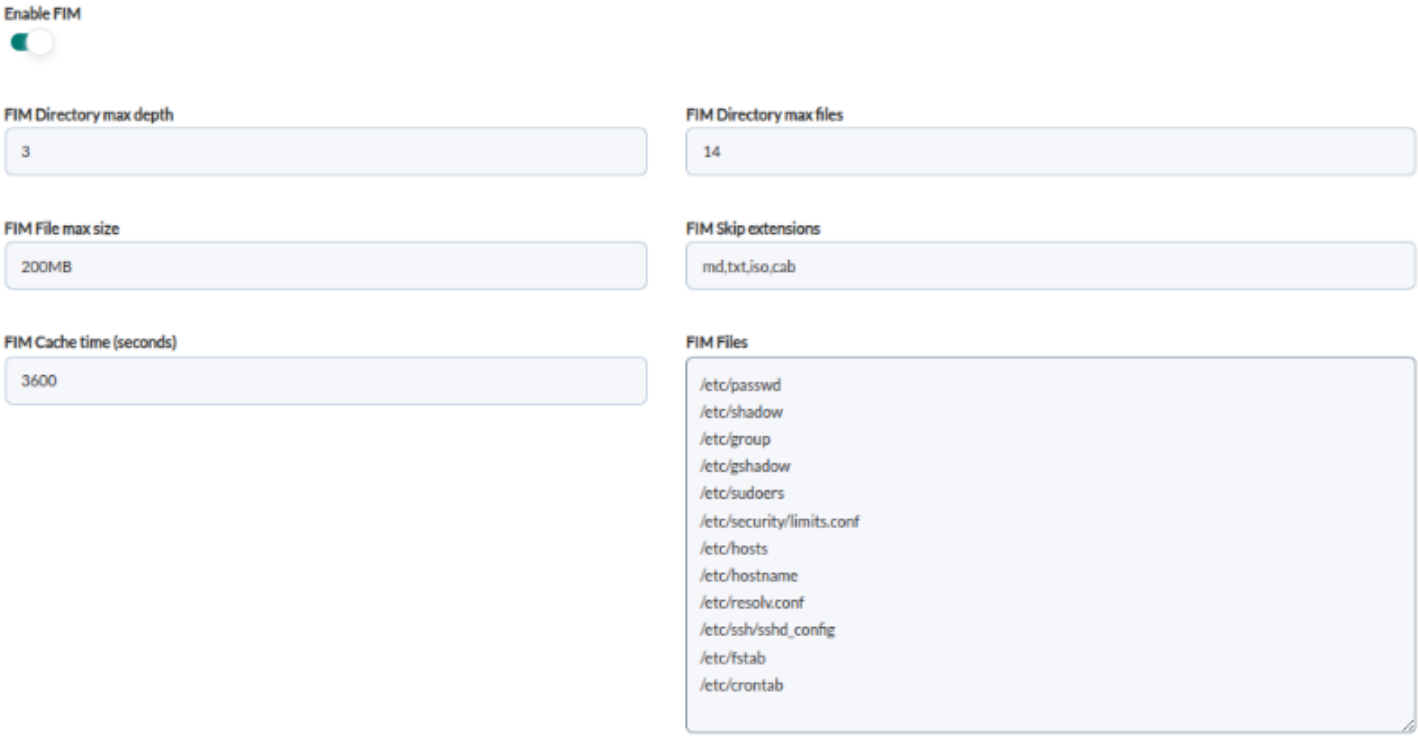
エージェントでの設定

エージェントのセキュリティ設定タブでは、FIM 監視を有効または無効にすることができます。

管理(Management) → リソース(Resources) → エージェント管理(Manage agents) → 編集(Edit) → セキュリティ(Security) → FIM を有効にする(Enable FIM)

この監視を有効にすると、エンドポイント 間隔ごとにチェックされる ファイルとディレクトリへのパス を指定できます。

設定ボックス（FIM ファイル(FIM files)）では、各行にファイルまたはディレクトリへのパスを指定する必要があります。各オペレーティングシステムにはデフォルト値があり、必要に応じて編集、削除、または追加できます（ポリシー設定も参照）。



指定されたすべてのパスについて、キャッシュ時間（秒単位）が保存されます（FIM キャッシュ時間(秒)(FIM Cache time(seconds))）。これは、ファイルが削除されたかどうかを判断するためのものです。つまり、指定された秒数を超えてシステムによって検出されない場合、ファイルは削除されたとみなされます。

ディレクトリへのパスの場合、そこに含まれるファイルの変更を検出するための特定のパラメータを指定することもできます。

- ファイルを検索するディレクトリ内の最大深度（サブディレクトリの数）を指定できます。
- 各ディレクトリで監視するファイルの最大数、ディレクトリ内のファイルの最大サイズ、および無視するファイル拡張子も指定できます。

最大ファイルサイズ（FIM ファイル最大サイズ(FIM File max size)）を指定するには、値と単位を入力します。無視する拡張子のリスト（FIM スキップする拡張子(FIM Skip extensions)）を指定するには、拡張子をカンマで区切ります。

FIM 検索に含めるファイル

ここでは、詳細に監視するファイルまたはディレクトリのリストを指定できます。これにより、ディレクトリ内の新規ファイル、消失ファイル、変更されたファイルを検出できます。最大深度パラメータとディレクトリパラメータで処理するファイルの最大数は、非常に一般的なディレクトリ（例：c:\Windows\System32）が入力された場合でも、エージェントがシステムリソースを過度に消費しないように設計されています。これらのパラメータはニーズに合わせて設定でき、分析対象のディレクトリとファイルのリストもカスタマイズできます。

特定のディレクトリやファイルを検索から除外する方法もあります。次に例を示します。

```
exclude /opt/myapp/*.tmp
```

または、各行の先頭に数字を追加してコメントを残すこともできます。そうすれば、コメントは考慮されず、必要に応じて有効にできます。

```
#exclude /opt/myapp/*.tmp
```

動的ディレクトリ (アスタリスク ワイルドカードを使用) は次のように検索に含めることができます。

```
C:\Users*\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\
```

監視ポリシー設定

個々のエージェント に対して行われるのと同じ設定が、監視ポリシー を通じて適用できます。

FIM 監視がポリシーから適用される場合、エージェントでこの設定を直接変更することはできません。

ポリシーを編集するときに、このオプションを有効にするタブが表示されます。

管理(Management) → 設定(Configuration) → ポリシー管理(Manage policies) メニューで、編集するポリシーの名前をクリックし、ファイル整合性監視(File Integrity Monitoring) → このポリシーから FIM を適用(Apply FIM from this policy) タブをクリックします。

このオプションに加えて、ポリシーエージェントに対して FIM を有効にするか無効にするかを指定する必要があります（オプションFIM を有効にする(Enable FIM)）。有効になっていない場合、FIM ポリシーの設定は実行されません。

これら最後の 2つのオプションを組み合わせることで、ポリシー自体からエージェントセットの FIM 監視を無効にすることができます。この場合、このポリシーから FIM を適用する(Apply FIM from this policy)を有効にし、FIM を有効にする(Enable FIM)を無効にする必要があります。

MS Windows® オペレーティングシステムにインストールされたエンドポイントの場合は、FIM files セクションを次のファイルに置き換える必要があります。

```
%SystemRoot%\System32\config\SAM
%SystemRoot%\System32\config\SYSTEM
%SystemRoot%\System32\config\SECURITY
```

```
%SystemRoot%\System32\config\SOFTWARE
%SystemRoot%\System32\config\DEFAULT
%SystemRoot%\System32\winlogon.exe
%SystemRoot%\System32\lsass.exe
%SystemRoot%\System32\services.exe
%SystemRoot%\System32\smss.exe
%SystemRoot%\System32\svchost.exe
%SystemRoot%\System32\csrss.exe
%SystemRoot%\System32\winload.exe
%SystemRoot%\System32\ntoskrnl.exe
%SystemRoot%\System32\drivers\etc\hosts
%SystemRoot%\explorer.exe
%SystemRoot%\System32\cmd.exe
%SystemRoot%\system32\WindowsPowerShell\v1.0\powershell.exe
%SystemRoot%\System32\wscript.exe
%SystemRoot%\System32\cscript.exe
%SystemRoot%\System32\taskmgr.exe
%SystemRoot%\SysWOW64\kernel32.dll
%SystemRoot%\SysWOW64\user32.dll
%SystemRoot%\SysWOW64\advapi32.dll
%SystemRoot%\SysWOW64\gdi32.dll
%SystemRoot%\SysWOW64\ntdll.dll
%SystemRoot%\SysWOW64\ole32.dll
%SystemRoot%\SysWOW64\shell32.dll
%SystemRoot%\SysWOW64\ws2_32.dll
%SystemRoot%\SysWOW64\cmd.exe
%SystemRoot%\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
%SystemRoot%\SysWOW64\wscript.exe
%SystemRoot%\SysWOW64\regsvr32.exe
%SystemRoot%\SysWOW64\mshta.exe
```

それ以外の場合、設定は エージェントに直接適用される設定 とまったく同じです。

FIM 監視結果

FIM 監視は、有効になっている各エージェントに次のモジュールを生成します。

- FIM_status: エージェントのファイル整合性が維持されているかどうかを監視します。
- FIM_status_last_change: FIM 監視状態の最終変更日。
- FIM_changed: 変更されたファイルの数を監視します。
- FIM_deleted: 削除されたファイルの数を監視します。
- FIM_new: 新しく見つかったファイルの数を監視します。

さらに、新規作成、変更、または削除されたファイルごとにログエントリが生成され、ログ収集 が有効になっている場合に表示できます。

SIEM との統合

FIM 監視は SIEM 監視 とも統合されています。Pandora FMS には、デフォルトで SIEM イベントを生成するためのデコーダーとルールが組み込まれています (ログ収集用に生成された ログエントリ に基づく)。

Pandora FMS ドキュメント一覧に戻る